Cybercrime moves to the cloud

Criminals in the information technology world have tapped into a new market for their attacks: the cloud. Just as businesses have begun to use cloud servers, criminals are shifting from usage of host computers, to a cloud server. It seems as though their victims are persons with large bank accounts. Not unlike typical bank fraud, the hackers send out a phishing email to a potential victim urging them to click a link and change their password. Malware from a cloud server is then downloaded onto the victim’s computer which then directs the user to the falsified website where a user name and password are entered. The cloud server takes all the information and sets up transfers automatically from the victim’s account to the hacker’s account, all while the victim believes the transfers are happening between their own accounts.

The biggest difference between the cloud attacks and the traditional host computer is automation. The servers have the ability to take user information and authenticate it against the users bank account almost instantly, eliminating much of the manual legwork. Researchers have discovered the servers are typically in eastern Europe with a “bullet-proof” ISP. Hackers rely on lax policies in these Eastern European countries and regular relocation to avoid recognition.

This just goes to prove, that as technology evolves, so do the criminals.

Two hackers plead guilty to LulzSec attacks on Web sites

Two members of the LulzSec hacking group plead guilty to the denial of service attacks launched on government and corporate Web sites. Ryan Cleary and Jake Davis used the name “Topiary” to attack the sites Sony, Nintendo, News International, Arizona State Police, HBGary, and PBS. The pair and several other hackers were charged with conspiracy and encouraging or assisting others to commit computer offenses and fraud. All plead not guilty to assisting, but Leary and Davis, along with an unnamed minor, plead guilty to conspiracy. The charges were brought about when stolen data was posted to public websites.

The trio is believed to be the founders of LulzSec. Another individual, Hector Xavier Monsegur, plead guilty and was released to become an informant. Monsegur’s information lead to the arrests. Many other members have been arrested relating to hacks on government and corporate sites